FAULT TOLERANT DESIGN

Practice:

Incorporate hardware and software features in the design of spacecraft equipment which tolerate the effects of minor failures and minimize switching from the primary to the secondary string. This increases the potential availability and reliability of the primary string.

Benefits:

Fault tolerant design provides a means to achieve a balanced project risk where the cost of failure protection is commensurate with the program resources and the mission criticality of the equipment. By providing compensation for potential hardware failures, a fault tolerant design approach may achieve reliability objectives without recourse to non-optimized redundancy or overdesign.

Programs That Certified Usage:

Voyager, Galileo, Magellan, Cassini

Center to Contact for Information:

Jet Propulsion Laboratory (JPL).

Implementation Method:

The practice of fault tolerant design (FTD) presumes that the potential causes of failures are identifiable. This identification is performed by means of the existing practices of hardware and software failure modes, effects, and criticality analysis (FMECA). Similarly, fault tree analysis (FTA) identifies safety issues and potential faults in mechanical and electromechanical devices. Design engineers utilize the preliminary results of FMECAs and FTAs to establish fault tolerant equipment design priorities.

FTD is an iterative process; its current validity relies on the current iteration of the FMECA and FTA and their corresponding criticalities and probabilities of occurrence. The iteration cycle ceases when either the cost of the next design iteration is programmatically unacceptable or when the risk has been reduced below a stated goal. It is assumed that all of the normal reliability design tools such as part stress derating, worst case performance analysis, qualification testing, life demonstration, quality control, etc., have already been used to preclude any design or material deficiencies. The FTD process also assumes that, in spite of the above practices, an in-flight failure may occur in a given set of manufactured hardware.

This process flow is illustrated in Figure 1. The diagram illustrates that FTD is a top-level system design philosophy covering other NASA preferred reliability practices, including analytical design disciplines, FMECA and FTA studies,

FAULT TOLERANT DESIGN

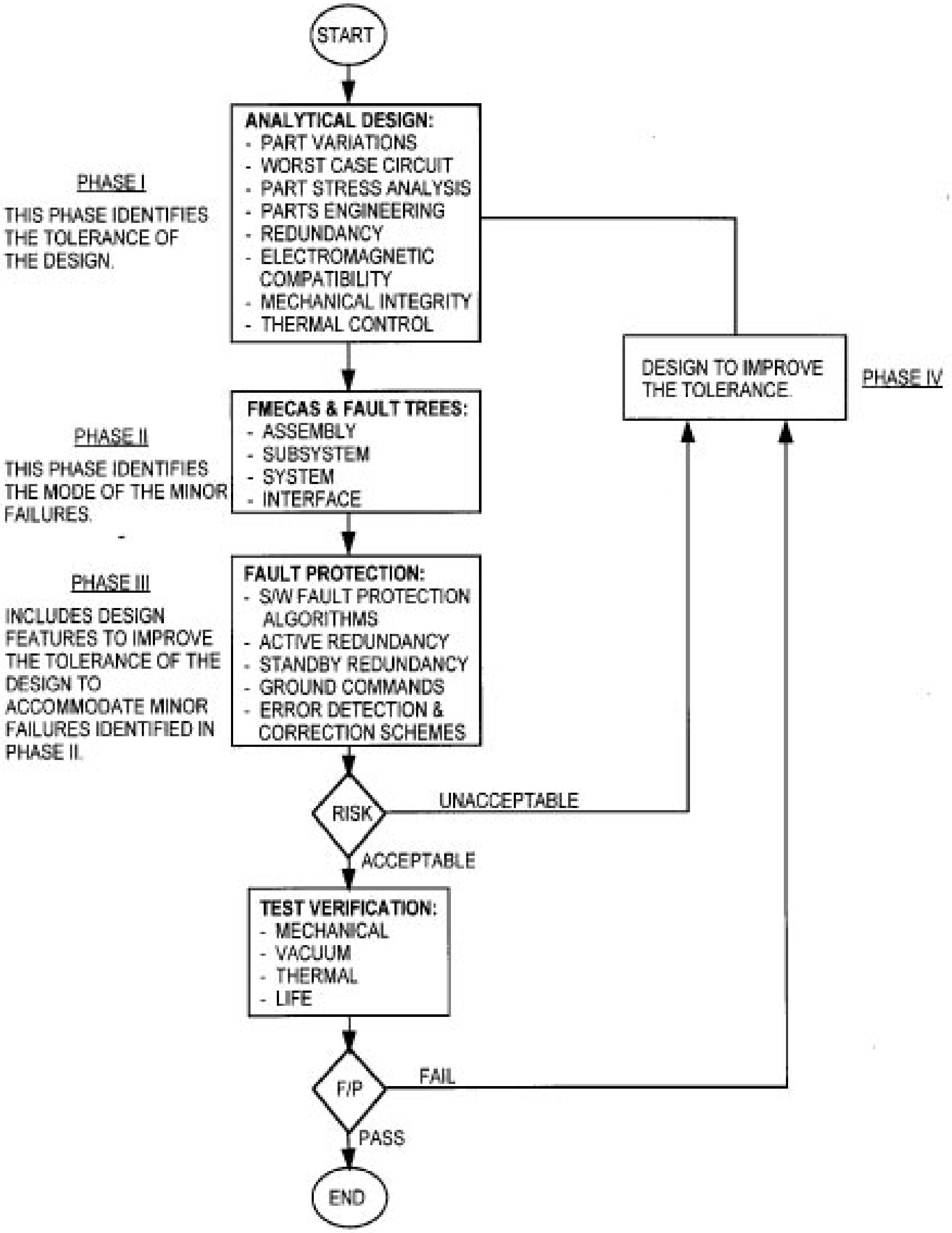

Figure 1: Process Flow Diagram for Fault Tolerant Design

fault protection plans, and test results. The FTD process at JPL includes four phases beginning with analytical design.

Technical Rationale:

To increase the reliability of a spacecraft system, two complementary but fundamentally different approaches are taken:

1. Fault prevention (fault intolerance), and
2. Fault tolerance.

Fault prevention deals with the objective of increasing reliability by elimination of all faults, which is not feasible in reality. Therefore, the goal of fault prevention is to reduce the probability of system failure to an acceptably low value.

The ***fault tolerance*** approach expects failures to occur. However, their effects will be automatically counteracted by incorporating either redundancy or other types of compensation.

A fault tolerant design approach differs from a pure design redundancy approach in that provisions are made for planned degraded modes of operation where acceptable. For example, the high gain antenna of a spacecraft is usually non-redundant because of its size. An FTD would favor the use of a backup medium gain antenna operating at reduced data rates as a degraded but acceptable operating mode. Similarly, a partially failed power source within a solar panel array or a failure of one of three radioisotope thermoelectric generators (RTGs) could be accommodated: an appropriate failure detection circuit and a software fault protection algorithm would be provided to shed low priority electrical loads or instruments, while maintaining most mission capabilities.

Also, FTD may be preferable to mere hardware redundancy in that higher probability multiple failures can be identified and accommodated. For example, the common design practice for inertial sensors (gyros) is the use of three packages of orthogonally located dual axis sensors (i.e., the X-Y, Y-Z, and Z-X axes). This scheme is tolerant of the loss of any one gyro but can be extended to accommodate the loss of any two gyros by the use of a pair of two-axis positionally adjustable gyros insertable by command or by detection algorithms. It can be placed in the X-Y or X-Z directions, thereby providing at least one signal on each axis even if two pairs of fixed mounted gyros are lost. In this case, dual failures are accommodated with only a short interruption of service and some additional mechanical complexity, but with no significant loss in system performance.

The essential ingredients to achieving a fault tolerant design are the performance of a thorough FMECA and FTA, the detailed communication of these identified failure modes and effects to the fault protection design engineers, and strong participation by the project engineer and program management in assessing design cost/benefit trade-off iterations. An FTD will be limited by either weight, volume, schedule, or cost constraints. Presentation of fault tolerant design options to

FAULT TOLERANT DESIGN

program management requires a skilled engineering team with intimate knowledge of system operation and close communication with system designers.

An FTD can provide dramatic improvements in system reliability and lead to a substantial reduction in flight failures as a consequence of fewer disabling system failures.

Impact of Non-Practice:

Systems which do not incorporate FTD as a part of their development process will experience a higher risk of a severely degraded or prematurely terminated mission, or it may result in excessively large weight volume, or high cost to achieve an acceptable level of performance by using non-optimized redundancy or overdesign.

Related Practices:

1. *Fault Protection*, Practice No. PD-ED-1243
2. *Active Redundancy*, Practice No. PD-ED-1216
3. *Failure Modes, Effects, and Criticality Analysis (FMECA)*, Practice No. PD-AP-1307

References:

1. *Fault Protection System Design and Operations,* JPL Document D625-505, Vol. 8, Galileo Project, October 1989.

2. *Fault Protection Requirements,* JPL Document 699-CAS-3-330, Cassini Project, March 1994.

3. *System Fault Protection Algorithms,* JPL Document 699-CAS-3-331, Cassini Project, January 1995.